CLAIMS

What is claimed is:

1.   A security method for transmission to a remote device of data input into a transaction terminal as clear text data, comprising the steps of:

(a)   comparing a data entry prompt for entry of data into the transaction terminal to prompts in a secure prompt table;

(b)   determining that the data entry prompt is a secure prompt upon the occurrence of any of the conditions of:

(i)   the data entry prompt matching at least one of the prompts in the secure prompt table,

(ii)   the data entry prompt matching only a portion of any of the secure prompts in the secure prompt table, and

(iii)   any of the prompts in the secure prompt table matching only a portion of the data entry prompt; and

(c)   transmitting the data entered into the transaction terminal in response to the data entry prompt as clear text data only upon the determination that the data entry prompt is a secure prompt.

2.   A security method for transmission to a remote device of data input into a transaction terminal as clear text data, comprising the steps of:

(a)   comparing a data entry prompt for entry of data into the transaction terminal to prompts in a secure prompt table;

5   (b)   determining that the data entry prompt is a secure prompt upon the occurrence of any of the conditions of:

(i)   the data entry prompt matching any prompt in the secure prompt table, and

(ii)   the data entry prompt matching only a portion of any 10   prompt in the secure prompt table; and

(c)   transmitting the data entered into the transaction terminal in response to the data entry prompt as clear text data only upon the determination that the data entry prompt is a secure prompt.

3.   The method of claim 2, wherein the step of determining that the data entry prompt is a secure prompt includes also doing so when any prompt in the secure prompt table matches only a portion of the data entry prompt.

4.   A security method for transmission to a remote device of data input into a transaction terminal as clear text data, comprising the steps of:

(a)   comparing a data entry prompt for entry of data into the transaction terminal to prompts in a secure prompt table;

(b)   determining that the data entry prompt is a secure prompt upon the occurrence of any of the conditions of:

(i)   the data entry prompt matching any prompt in the secure prompt table, and

(ii)   any prompt in the secure prompt table matching only a portion of the data entry prompt; and

(c)   transmitting the data entered into the transaction terminal in response to the data entry prompt as clear text data only upon the determination that the data entry prompt is a secure prompt.

5.   The method of claim 4, wherein the step of determining that the data entry prompt is a secure prompt includes also doing so when the data entry prompt matches only a portion of any prompt in the secure prompt table.

6.   In a personal identification number entry device, a clear text data transmission security method, comprising the steps of:

(a)   the personal identification number entry device receiving a data entry prompt for the entry of data from a remote device followed by a command from the remote device for entry of data into the personal identification number entry device;

(b)   the personal identification number entry device comparing the data entry prompt to a plurality of secure prompts and determining that the data entry prompt is a secure prompt upon the occurrence of any of the conditions of

(i)   the data entry prompt matching any of the secure prompts, and

(ii)   the data entry prompt matching only a portion of any of the secure prompts;

(c)   the personal identification number entry device accepting the data entry command only upon the determination that the data entry prompt is a secure prompt.

7.   The method of claim 5, wherein the step of determining that the data entry prompt is a secure prompt includes also doing so when any of the secure prompts matches only a portion of the data entry prompt.

8.   In a personal identification number entry device, a clear text data transmission security method, comprising the steps of:

(a)   the personal identification number entry device receiving a data entry prompt for the entry of data from a remote device followed by a command from the remote device for entry of data into the personal identification number entry device;

(b)   the personal identification number device comparing the data entry prompt to a plurality of secure prompts and determining that the data entry prompt is a secure prompt upon the occurrence of any of the conditions of:

(i)   the data entry prompt matching any of the secure prompts, and

(ii) any of the secure prompts matching only a portion of the data entry prompt; and

(c)   the personal identification number device accepting the data entry command only upon the determination that the data entry prompt is a secure prompt.

9.   The method of claim 8 wherein the step of determining that the data entry prompt is a secure prompt includes also doing so when the data entry prompt matches only a portion of any of the secure prompts.

10.   In a data entry device that displays a data entry prompt received from a remote device and transmits data input into the data entry device in response to the data entry prompt as clear text data only if the data entry prompt is a secure prompt, an improved method of determining whether the data entry prompt is a secure prompt, comprising the steps of:

(a)   comparing the data entry prompt with prompts in a secure prompts table; and

(b)   determining that the data entry prompt is a secure prompt upon the occurrence of any of the conditions of:

(i)   the data entry prompt matching any prompt in the secure prompt table,

(ii)   the data entry prompt matching only a portion of any prompt in the secure prompt table, and

(iii)   any prompt in the secure prompt table matching only a portion of the data entry prompt.

11.   The method of claim 10 wherein the data entry device comprises a personal identification number entry device.

12.   In a personal identification number entry device that displays a data entry prompt received from a remote device and transmits data input into the data entry device in response to the data entry prompt as clear text data only if the data entry prompt is a secure prompt, an improved method of determining whether the data entry prompt is a secure prompt, comprising the steps of:

(a)   storing a plurality of secure prompts in a secure prompt table in memory of the personal identification number entry device;

(b)   comparing the data entry prompt with the secure prompts stored in the secure prompt table; and

(c)   determining that the data entry prompt is a secure prompt upon the occurrence of any of the conditions of:

(i)   the data entry prompt matching any secure prompt in the secure prompt table,

(ii)   the data entry prompt matching only a portion of any secure prompt in the secure prompt table, and

(iii)   any secure prompt in the secure prompt table matching only a portion of the data entry prompt.